UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN

CRYSTAL MARTINEZ and TIFFANY PARRISH, *on behalf of themselves and all others similarly situated*, Plaintiffs, v. MENTAVI, INC., ADHD ONLINE, LLC and ADHD ONLINE LLC d/b/a MENTAVI HEALTH Defendants.	Case No. 1:25-cv-228 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Crystal Martinez and Tiffany Parrish, individually and on behalf of all others similarly situated, by and through undersigned counsel, hereby allege the following against Mentavi, Inc., ADHD Online, LLC and ADHD Online, LLC d/b/a/ Mentavi Health ("Defendants" or "ADHD Online"). Facts pertaining to Plaintiffs and their experiences and circumstances are alleged based upon personal knowledge, and all other facts alleged herein are based upon due investigation of counsel and—where indicated—upon information and good faith belief.

INTRODUCTION

1. Information concerning a person's physical and mental health is among the most confidential and sensitive information in our society and the mishandling of such information can

have serious consequences including, but certainly not limited to, discrimination in the workplace or denial of insurance coverage.[1]

2. Simply put, if people do not trust that their sensitive private medical information will be kept private and secure, they may be less likely to seek medical treatment which can lead to more serious health consequences down the road. Because of this, protecting the confidentiality of medical information and preventing its unauthorized disclosure is vital to maintaining public trust in the healthcare system as a whole.

3. The need for data privacy, security and transparency is particularly acute when it comes to the rapidly expanding world of digital telehealth providers; of all the information the average internet user shares with technology companies, health data is some of the most extensive, valuable and controversial.[2]

4. ADHD Online is a telehealth company that connects patients and prospective patients with clinicians and therapists for online mental health diagnosis and treatment of attention-deficit/hyperactivity disorder ("ADHD").

---

[1] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized.").

[2] Protected and highly sensitive medical information collected by telehealth companies includes many categories from intimate details of an individual's conditions, symptoms, diagnoses and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. *See* Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020) https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137.

5. In order to market, sell and provide these services, Defendants own, control and maintain the website https://adhdonline.com/ which contains a patient portal, available at https://patients.adhdonline.com (the "Website"), which require individuals to share highly sensitive personally identifiable information ("PII") and protected health information ("PHI") in order to review treatments for specific medical conditions (such as ADHD and ADHD-related anxiety, depression and binge eating), create accounts, participate in health screenings and receive treatments.

6. In order to acquire the highly valuable PHI and PII of its patients and prospective patients (the "Users"), ADHD Online installed tracking technologies including, but not limited to, the Meta Pixel (the "Pixel"), Google Analytics and Google DoubleClick ("Tracking Tools") on their Website.[3]

7. Invisible to the naked eye, Tracking Tools—which are configured by the website owner, here, ADHD Online—collect and transmit information from Users' browsers to unauthorized third parties including, but not limited to, Meta Platforms, Inc. d/b/a Facebook and Google, Inc. ("Google").

8. One of the Tracking Tools ADHD Online deployed on their Website is the Meta Pixel ("Pixel"). The Pixel is a snippet of code that, when embedded on a website, tracks the website visitor's activity on that website and sends that data to a third party, like Meta. [4]

[3] Other trackers ADHD Online installed on its Web Properties include Microsoft Clarity, which can be used as a session replay tool, and Microsoft Bing.

[4] Google Analytics is one of Google's tracking technologies comparable to the Meta Pixel. Meta also provides other tracking technologies that give the same or similar tracking functionalities as the Pixel including, but not limited to, Conversions API, SDKs, and Audiences. Absent discovery, Plaintiffs are unable to independently confirm whether Defendant installed such tracking technologies on its Web Properties.

9. The process of adding third-party trackers such as the Tracking Tools to webpages is a multi-step process that must be undertaken *by the website owner*.[5]

10. Aside from the various steps to create and activate the Pixel, website owners must also agree to Facebook's Business Tools Terms by which Facebook requires website owners using the Meta Pixel to "represent and warrant" that they have adequately and prominently notified users about the collection, sharing and usage of data through Facebook's Business Tools and that websites "will not share Business Tool Data . . . that [websites] know or reasonably should know . . . includes health, financial information or other categories of sensitive information . . . ."[6]

11. Website owners using Google Analytics must comply with Google's terms and policies, which require them to prominently disclose their use of Google Analytics and provide information about how data is collected and processed. Additionally, website owners must ensure that they do not transmit personally identifiable information (PII) or sensitive data to Google

---

[5] *Business Help Center: How to set up and install a Meta Pixel*, https://www.facebook.com/business/help/952192354843755?id=1205376682832142; *see* Ivan Mana, *How to Set Up & Install the Facebook Pixel (in 2022)*, https://www.youtube.com/watch?v=ynTNs5FAUm8; *Add Your Google Analytics (GA4) Tracking Code*, https://www.pixelyoursite.com/documentation/add-your-google-analytics-code.

While the Meta Pixel as well as other trackers may be small (and, in fact, invisible pieces of code), the data they collect and transmit is extremely extensive. *See Meta for Developers: Meta Pixel*, https://developers.facebook.com/docs/meta-pixel/.

[6] *Meta Business Tools Terms*, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfbOvnb7E0sZ-wzgCW6xNLFKEOEVH_fr6JjkMINTJNqN7i1R-3MPh5caFgmdgAOxbL8&_rdr ("When you use any of the Meta Business Tools to send us or otherwise enable the collection of Business Tool Data . . . , these Business Tools Terms govern the use of that data"); *see also* Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report*, NEWS BYTE (June 16, 2022), https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story (quoting Facebook spokesman Dale Hogan as saying that it is "against [Facebook's] policies for websites and apps to send sensitive health data about people through [its] Business Tools").

Analytics, such as names, email addresses, social security numbers, or any other information that can permanently identify an individual or their device. These requirements are designed to protect user privacy and ensure that data collection practices align with Google's policies and legal standards.[7]

12. Google stores users' logged-in identifiers on a non-Google website in its logs. Whenever a user logs-in on non-Google websites—whether in private browsing mode or non-private browsing mode—the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses this data to serve personalized ads, among other things.

13. The Tracking Tools prompt users' web browsers to transmit specific information based on parameters set by the website owner. This customizable nature of tracking codes allows the website owner to determine which webpages contain the Tracking Tools, and which events and user actions are tracked and shared with Facebook or Google.

14. Consequently, by implementing the Tracking Tools on their Website, ADHD Online introduced third-party trackers onto the web browsers of its Users, enabling real-time disclosure of their communications to Facebook and Google as they are transmitted to ADHD Online.

15. Here, despite the fact that ADHD Online unquestionably used the Tracking Tools to acquire its Users' PHI and PII, it did ***not*** notify those Users about the surreptitious collection of their sensitive data.

[7] *Google Analytics Terms of Service*, https://support.google.com/analytics/answer/7318509.

16. Once Users' PHI and PII is collected and transmitted to, for example Facebook, it is combined with a User's Facebook profile and all the information about this person is accessible via the User's unique Facebook ID.

17. Facebook tracks and collects data even on people who do not have a Facebook account or have deactivated their Facebook accounts. Those individuals can find themselves in an even worse situation because even though their PHI and PII is sent to Facebook—without their consent—they cannot clear past activity or disconnect the collection of future activity since they do not possess an account (or an active account).[8]

18. Google's tracking technologies operate much like the Meta Pixel. As one District Court recently described:

> Whenever a user visits a website that is running Google Analytics, Ad Manager, or some similar Google service, Google's software directs the user's browser to send a separate communication to Google. . . . When a user visits a website, the user's browser sends a "GET" request to the website to retrieve it. This GET request contains the following information: the Request URL, or the URL of the specific webpage the user is trying to access; the user's IP address; the User-agent, which identifies the user's device platform and browser; user's geolocation, if available; the Referer, which is the URL of the page on which the user clicked a link to access a new page; event data, which describes how users interact with a website, for example, whether they saw an ad or played a video; and the actual search queries on the site. At the same time, the user's browser reads Google's code, which is embedded on the website. Google's code instructs the user's browser to send a second and concurrent transmission directly to Google. This second transmission tells Google exactly what a user's browser communicated to the website.[9]

[8] In the past, these were referenced as "ghost accounts" or "shadow profiles." *See* Laura Hautula, *Shadow profiles: Facebook has information you didn't hand over*, CNET (April 11, 2018), https://www.cnet.com/news/privacy/shadow-profiles-facebook-has-information-you-didnt-hand-over/.

[9] *Brown v. Google LLC*, 685 F. Supp. 3d 909, 919–20 (N.D. Cal. 2023). As explained by the Court in *Brown*, Google connects user data to IP addresses; IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifiable information that constitutes one of the 18 HIPAA identifiers of PHI. *See* 45 C.F.R. § 164.514 (2).

19. Then, completely unencumbered by any pretense of restriction or regulation, Facebook and Google, in turn, use that PHI and PII for various business purposes, including using such information to "improve" advertisers' ability to target specific demographics and selling such information to third-party marketers who target those users online (through their Facebook, Instagram, Gmail and other social media and personal accounts):

> Along with encouraging businesses to spend ad dollars, Facebook also receives the transmitted data, and can use it to hone its algorithms. Facebook can also use data from the pixel to link website visitors to their Facebook accounts, meaning businesses can reach the exact people who visited their sites. The pixel collects data regardless of whether the visitor has an account.[10]

20. Healthcare patients simply do not anticipate that their trusted healthcare provider will send PHI and PII collected via its web pages to undisclosed third parties—let alone Facebook and Google, which have a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without their informed and express consent.[11]

21. But, although ADHD Online's patients understandably had a reasonable expectation of privacy as they used the Website, those Users were unknowingly providing their PHI and PII to ADHD Online as they (i) navigated the Website, (ii) reviewed specific medical

[10] *See* Colin Lecher & Ross Teixeira, *Facebook Watches Teens Online As They Prep For College* (Nov. 22, 2023), https://themarkup.org/pixel-hunt/2023/11/22/facebook-watches-teens-online-as-they-prep-for-college.

[11] This Court will not have to look far to find evidence of Meta's and Google's violations of privacy laws. In 2023 the European Union fined Meta "a record-breaking" $1.3 billion for violating EU privacy laws, and Google $400 million in 2022 for similar violations. *See* Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, CNN (May 22, 2023), https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html; *see* Kendra Barnett, *Google's $400M Penalty: The Impact of the 5 Heftiest Data Privacy Fines on 2023 Ad Plans*, The Drum (Nov. 15, 2022), https://www.thedrum.com/news/2022/11/15/googles-400m-penalty-the-impact-the-5-heftiest-data-privacy-fines-2023-ad-plans.

conditions and available treatments, (iii) created patient accounts and (iv) completed health assessments and questionnaires including their medical histories.

22. Plaintiffs and Class Members who visited and used ADHD Online's Website thought they were communicating *only* with their trusted healthcare provider. But by employing Tracking Tools—which obtain detailed information about its Users' medical information (including highly sensitive categories such as mental health)—ADHD Online effectively traded the private medical information of its patients for detailed analytics of its Users to increase its revenues and profits.

23. To make matters worse, ADHD Online has ***not*** informed those Users of the unauthorized disclosure of their PHI and PII, as many other healthcare and telehealth entitles who have utilized similar tracking technology to collect and disclose PHI and PII to third parties have done.[12]

24. Upon information and belief, ADHD Online also installed and implemented the Facebook Conversions Application Programming Interface ("Conversions API") on the Website. Conversions API serves the same purpose as the Meta Pixel in that it surreptitiously collects and transmits Users' PHI and PII to Facebook. Unlike the Meta Pixel, however, Conversions API functions from Defendant's servers and therefore cannot be stymied by use of anti-Pixel software

[12] In stark contrast to ADHD Online, in the past couple of years several medical providers that installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf; Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies,* FIERCE HEALTHCARE (October 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWSWIRE (August 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

or other workarounds. ADHD Online secretly enabled additional unauthorized transmissions and disclosures of Plaintiffs' and Class Members' Private Information to Facebook by implementing the Conversions API.

25. Thus, operating as implemented by ADHD Online, the Meta Pixel, Conversions API and other tracking technologies allow the PHI and PII that Plaintiffs and Class Members submit in confidence to be unlawfully disclosed to Facebook alongside the individual's name and other identifying information, including his or her Facebook ID, IP addresses and other identifying information pertaining to any accounts they may have with Facebook. This surreptitious and illegal collection and divulgence occurs on every webpage in which ADHD Online installed the Meta Pixel and for which it enabled Conversions API.

26. Despite numerous warnings from federal regulators (not to mention several FTC enforcement actions against telehealth companies for similar conduct) about the data privacy risks of using third-party tracking technologies,[13] ADHD Online designed and maintained their Website so that Users would be required to submit PHI and PII in order to participate in health assessments and other health-related services, review treatments offered by ADHD Online for their medical conditions, purchase treatment options and create accounts, among many other things.

27. The reason ADHD Online goes to these lengths to obtain this sensitive PHI and PII is, quite simply, because its Users would ***not*** provide it if they were informed and given a choice.

[13] *See, e.g.*, Heather Landi, *Regulators Warn Hospitals and Telehealth Companies about privacy risks of Meta, Google Tracking Tech*, FIERCE HEALTHCARE (July 21, 2023), https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google (noting that the FTC and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) issued a rare joint release announcing that 130 hospital systems and telehealth providers received a letter warning them about the data privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps).

That is, if ADHD Online told its patients that by using their Website their sensitive PHI and PII would be collected and disseminated to Facebook, Google or other third-party data brokers, Users would deny consent or demand significant compensation for the use of their private and valuable health information in this manner.

28. As detailed herein, ADHD Online owed common law, contractual, statutory and regulatory duties to keep Users' PHI and PII safe, secure and confidential. Furthermore, by obtaining, collecting, using and deriving a benefit from their PHI and PII, ADHD Online assumed legal and equitable duties to Users to protect and safeguard their PHI and PII from unauthorized disclosure.

29. ADHD Online, however, failed in its obligations and promises by utilizing the Tracking Tools to collect and divulge Users' PHI and PII to unauthorized third parties such as Facebook and Google.[14]

30. Given the nature of Facebook and Google's businesses as two of the world's largest online advertising companies, Plaintiffs' and Class Members' PHI and PII can and will likely be further used by or exposed to additional third parties.

31. As a result, Plaintiffs and Class Members have suffered numerous compensable injuries including (i) invasion of privacy, (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the transmissions of their PHI and PII to

[14] ADHD Online breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure the Web Properties were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share patients' PHI and PII; (iii) failing to obtain the consent of patients, including Plaintiffs and Class Members, to disclose their PHI and PII to Facebook, Google or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' PHI and PII through the Tracking Technologies; (v) failing to warn Plaintiffs and Class Members of such sharing and disclosures and (vi) otherwise failing to design and monitor the Web Properties to maintain the confidentiality and integrity of patients' PHI and PII.

Facebook or Google, (iii) loss of the benefit of the bargain, (iv) diminution of value of their disclosed PHI and PII, (v) statutory damages and (vi) the continued and ongoing risk to their PHI and PII.

32. Plaintiffs seek to remedy these harms and therefore bring this class action lawsuit on behalf of all similarly situated individuals to recover for harms suffered and assert the following claims: (i) Violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511; (ii) Negligence; (iii) Breach of Implied Contract; (iv) Breach of Confidence; and (v) Unjust Enrichment.

PARTIES

33. Plaintiff Crystal Martinez is a citizen of the State of Tennessee residing in Marshall County, where she intends to remain.

34. Plaintiff Tiffany Parrish is a citizen of the State of Georgia residing Worth County, Georgia where she intends to remain.

35. Defendant Mentavi, Inc. is a Delaware corporation with its principal place of business at 625 Kenmoor Ave., SE, Suite 301, Grand Rapids, Michigan.

36. Defendant ADHD Online, LLC is a Michigan corporation with its principal place of business at 625 Kenmoor Ave., SE, Suite 301, Grand Rapids, Michigan.

37. Defendant ADHD Online, LLC d/b/a Mentavi Health is a Delaware corporation with its principal place of business at 625 Kenmoor Ave., SE, Suite 301, Grand Rapids, Michigan.

38. Defendants ADHD Online, LLC and ADHD Online, LLC d/b/a Mentavi Health share the same corporate headquarters as Defendant Mentavi, Inc. in Grand Rapids, Michigan.

39. Upon information and belief, Mentavi, Inc. does business as Mentavi Health.

40. Upon information and belief, ADHD Online, LLC and ADHD Online, LLC d/b/a Mentavi Health are wholly owned subsidiaries of Mentavi, Inc.

41. Upon information and belief, all defendants are jointly and severally liable for the conduct alleged herein and acted in concert and as agents for one another in taking the actions giving rise to liability herein.

JURISDICTION & VENUE

42. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because this Complaint asserts a claim for violation of federal law, specifically, the ECPA, 18 U.S.C. § 2511. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

43. This Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) ("CAFA") as the amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than ADHD Online.

44. This Court has personal jurisdiction over Defendant because they operate and maintain their principal place of business in this judicial district. Further, Defendant is authorized to and regularly conducts business in this judicial district and makes decisions regarding corporate governance and management of the Website in this judicial district including, but not limited to, decisions regarding the privacy and security of Users' PHI and PII and the incorporation of Tracking Tools.

45. Venue is proper in this judicial district under 28 U.S.C. § 1391(a) through (d) and 28 U.S.C. § 101(b) for the following reasons: (i) a substantial part of the events giving rise to this

action occurred in this judicial district including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiffs' and Class Members' PHI and PII; (ii) Defendant's principal place of business is located in this judicial district; (iii) Defendant collects and redistributes Class Members' PHI and PII in this judicial district and (iv) Defendant caused harm to Class Members residing in this judicial district.

COMMON FACTUAL ALLEGATIONS

A. Federal Regulators Have Warned Healthcare Providers About the Impermissible Use of Tracking Technologies.

46. This surreptitious collection and divulgence of PHI and PII is an extremely serious data security and privacy issue. Both the Federal Trade Commission and the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS") have reiterated the importance of and necessity for data security and privacy concerning health information.

47. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information.***"[15]

[15] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* FTC Business Blog (July 25, 2023) (emphasis added), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.

48. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***
>
> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information***.[16]

49. HHS affirmed that HIPAA and its regulations prohibit the transmission of individually identifiable health information ("IIHI") by tracking technology like Google Analytics and the Meta Pixel without the patient's authorization and other protections like a business associate agreement with the recipient of patient data.[17]

---

[16] *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization.

[17] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (noting that "IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.").

On June 20, 2024, this guidance was vacated *in part* by Judge Pittman of in the Northern District

50. The federal government is taking these violations of health data privacy and security seriously as recent high-profile FTC settlements against several telehealth companies evidence. For example, the FTC imposed a $1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive PHI with advertising companies and platforms, including Facebook, Google and Criteo, and a $7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared customer health data with Facebook and Snapchat for advertising purposes. And Easy Healthcare was ordered to pay a $100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app Premon shared health data for advertising purposes.[18]

---

of Texas due to the court finding it in part to be the product of improper rulemaking and it is cited for reference only until the OCR updates its guidance, should it do so in the future. *See American Hosp. Ass'n. v. Becerra*, 738 F. Supp. 3d 780 (N.D. Tex. 2024). Notably, the court's order found *only* that the OCR's guidance regarding covered entities disclosing to third parties users' IP addresses while those users navigated *unauthenticated public webpages* ("UPWs") was improper rulemaking. The Order in no way affects or undermines the OCR's guidance regarding covered entities disclosing personal identifiers, such as Google or Facebook identifiers, to third parties while patients were making appointments for particular conditions, paying medical bills or logging into (or using) a patient portal. *See id*. at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the "Proscribed Combination" defined as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers" but stating that "[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document."). The FTC bulletin on the same topics remains untouched as do the FTC's enforcement actions against healthcare providers for committing the same actions alleged herein)..

[18] *See How FTC Enforcement Actions Will Impact Telehealth Data Privacy*, Health IT Security, https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy; *see* Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), www.law360.com/articles/1571369/ftc-targets-goodrx-in1st-action-under-health-breach-rule?copied=1 ("The Federal Trade Commission signaled it won't hesitate to wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale."); https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising; https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc.

51. In July 2023 federal regulators sent a letter to approximately 130 healthcare providers warning them about using online tracking technologies that could result in unauthorized disclosures of PHI and PII to third parties. The letter highlighted the "risks and concerns about the use of technologies, such as the Meta Pixel and Google Analytics, that can track a user's online activities," and warned about "[i]mpermissible disclosures of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others." According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[19]

52. Moreover, the Office for Civil Rights at HHS has made clear, in a recent bulletin titled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the transmission of such protected information violates HIPAA's Privacy Rule:

---

[19] *See* https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.

On June 20, 2024, this guidance was vacated *in part* by Judge Pittman of in the Northern District of Texas due to the court finding it in part to be the product of improper rulemaking and it is cited for reference only until the OCR updates its guidance, should it do so in the future. *See American Hosp. Ass'n. v. Becerra*, 738 F. Supp. 3d 780 (N.D. Tex. 2024). Notably, the court's order found *only* that the OCR's guidance regarding covered entities disclosing to third parties users' IP addresses while those users navigated *unauthenticated public webpages* ("UPWs") was improper rulemaking. The Order in no way affects or undermines the OCR's guidance regarding covered entities disclosing personal identifiers, such as Google or Facebook identifiers, to third parties while patients were making appointments for particular conditions, paying medical bills or logging into (or using) a patient portal. *See id*. at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the "Proscribed Combination" defined as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers" but stating that "[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document."). The FTC bulletin on the same topics remains untouched as do the FTC's enforcement actions against healthcare providers for committing the same actions alleged herein).

> **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[20]

53. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to monetize their users' PHI and PII.

54. For instance, THE MARKUP reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.[21]

55. And, in the aptly titled report *"Out of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation by STAT and THE MARKUP of 50 direct-to-consumer telehealth companies reported that telehealth companies or virtual care websites were providing sensitive medical information they collect to the world's largest advertising platforms.[22]

---

[20] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, *supra*, n. 17.

[21] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[22] Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools*, The Markup (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies .

56. Many telehealth sites had at least one tracker—from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn and Pinterest—that collected patients' answers to medical intake questions.[23]

B. The Meta Pixel

57. Meta's core business function is to sell advertising, and it does so on several platforms, including Facebook and Instagram. The bulk of Meta's billions of dollars in annual revenue comes from advertising—a practice in which Meta actively participates by using algorithms that approve and deny ads based on the ads' content, human moderators that further review ads for both legality and aesthetics prior to and after the ads are published, and other algorithms that connect ads to specific users, without the assistance or input of the advertiser.

58. Over the last decade, Meta has become one of the largest and fastest growing online advertisers in the world. Since its creation in 2004, Facebook's daily, monthly, and annual user base has grown exponentially to billions of users.

59. Meta's advertising business has been successful due, in significant part, to its ability to target users, both based on information users provide to Meta, and based on other information about users Meta extracts from the Internet at large. Given the highly specific data used to target particular users, thousands of companies and individuals utilize Facebook's advertising services.

60. One of Meta's most powerful advertising tools is the Meta Pixel, which it first launched as the Facebook Pixel in 2015.

[23] *See id.* (noting that "[t]rackers on 25 sites, including those run by industry leaders Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan").

61. The Pixel is an easily attainable piece of code that Meta makes available to website developers for free. In exchange, at a minimum, website developers must agree to Meta's Business Tool Terms.[24]

62. The Business Tools Terms note that the Meta's Business Tools including the Pixel capture two types of information: "Contact Information" which "personally identifies individuals," and "Event Data" which contains additional information about people and their use of a developer's website.[25]

63. The Business Tools Terms also require websites to "provide[] robust and sufficiently prominent notice to users . . . on each web page where our pixels are used that links to a clear explanation (a) that third parties, including Meta, may . . . collect or receive information from your websites and elsewhere on the Internet and use that information to . . . deliver ads, (b) how users can opt out of the collection and use of information . . . and (c) where a user can access a mechanism for exercising such choice[.]"[26]

64. Even with these protocols in place, Meta prohibits the disclosure of Business Tools Data "that you know or reasonably should know . . . includes health, financial information or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines)."[27]

---

[24] *See* Meta Business Tool Terms, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zuI0STn-VURAyVhvlzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr ("When you use any of the Meta Business Tools . . . or otherwise enable the collection of Business Tool Data . . . these Business Tool Terms govern the use of that data").

[25] *Id.*, § 1(a)(i)-(ii).

[26] *Id.*, § 3(c)(i).

[27] *Id.*, § 1(h).

65. After agreeing to the Business Tools Terms, website developers can choose to install and use the Pixel on their websites to track and measure certain actions, such as a website visitor's text searches and page views, including the detailed URLs triggered by page views.

66. The Pixel "tracks the people and the types of actions they take."[28] According to Meta, the Pixel is a piece of code that allows Defendant to measure the effectiveness of [its] advertising by understanding the actions [website visitors] take on [its] website."[29]

67. When a website visitor takes an action a developer chooses to track on its website, the Pixel is triggered and sends data about that "Event" to Meta. All of this happens without the user's knowledge or consent.

68. Thus, by secretly recording and transmitting data to Meta—without the user's knowledge or consent—the Pixel acts much like a traditional wiretap controlled by Defendant.

69. Through this online tracking technology, Meta intercepts each page a user visits, what buttons they click, as well as the specific information the user inputs into the website and other searches conducted. The Pixel sends each of these pieces of information to Meta with PII, including the user's unique identifiers from Meta and their IP address. Meta stores this data on its own servers, in some instances for years on end, and independently uses the data for its own financial gain.

C. ADHD Online's Method of Transmitting PHI and PII.

70. In order to use its online services, customers must provide ADHD Online PHI and PII on their Website.

---

[28] *Retargeting*, https://www.facebook.com/business/goals/retargeting.

[29] *About Meta Pixel*, Meta Business Help Center, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

71. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (computer, tablet or smartphone) accesses web content through a web browser (*e.g.*, Google's Chrome, Mozilla's Firefox, Apple's Safari, or Microsoft's Edge browsers).

72. Every website is hosted by a computer "server" that holds the website's contents. The entity(ies) in charge of the website exchange communications with users' client devices as their web browsers query the server through the internet.

73. Web communications consist of Hypertext Transfer Protocol ("HTTP") or Hypertext Transfer Protocol Secure ("HTTPS") requests and HTTP or HTTPS responses, and any given browsing session may consist of thousands of individual HTTP requests and HTTP responses, along with corresponding cookies:

a. **HTTP request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF to file a motion to a court.)

b. **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.

c. **HTTP response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP request. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data.

74. A patient's HTTP request essentially asks ADHD Online's Website to retrieve certain information (such as a set of health screening questions). The HTTP response sends the

requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons and other features that appear on the participants' screens as they navigate ADHD Online's Website.

75. Every website is comprised of Markup and source code. Source code is a simple set of instructions that commands the website user's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

76. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP requests quietly executed in the background without notifying the web browser's user.

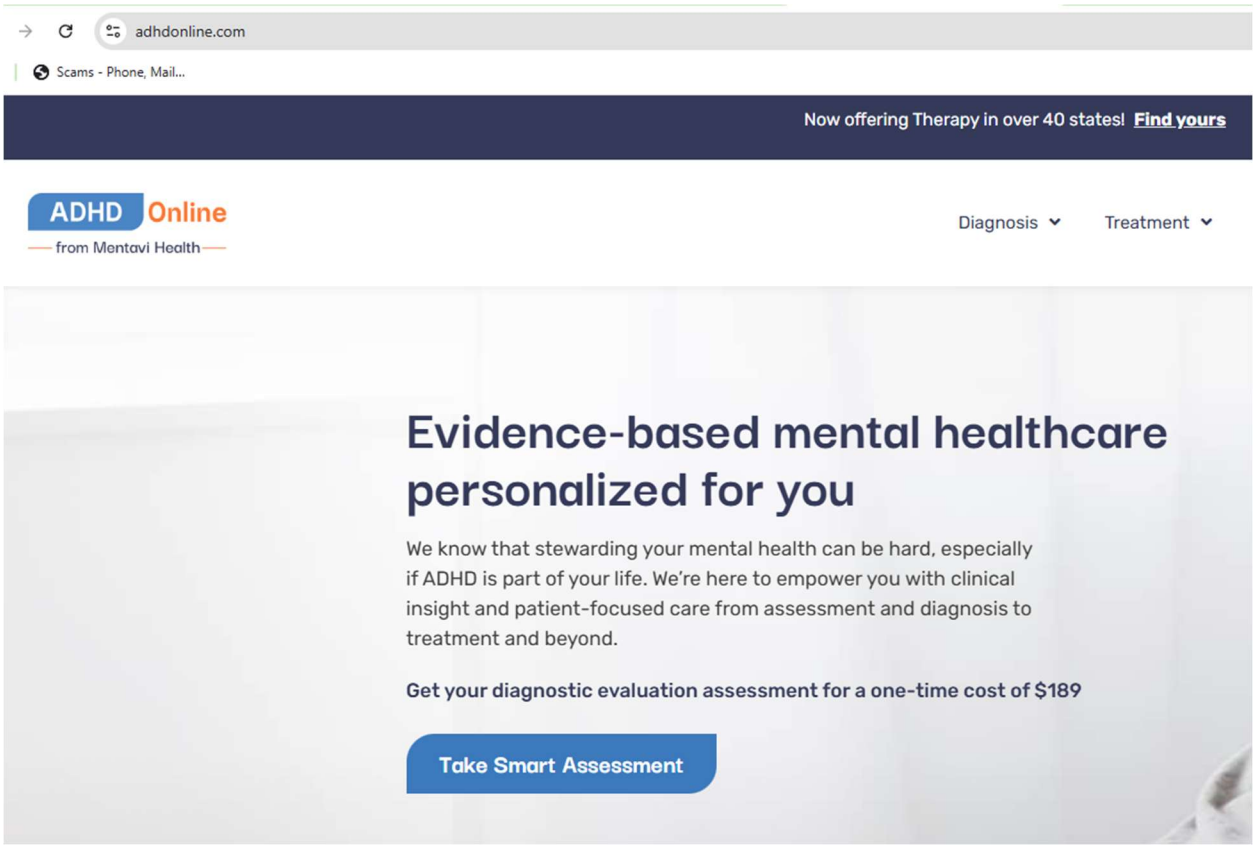
77. The Tracking Tools are source code that do just that—they surreptitiously transmit a Website User's communications and inputs to Meta and Google.

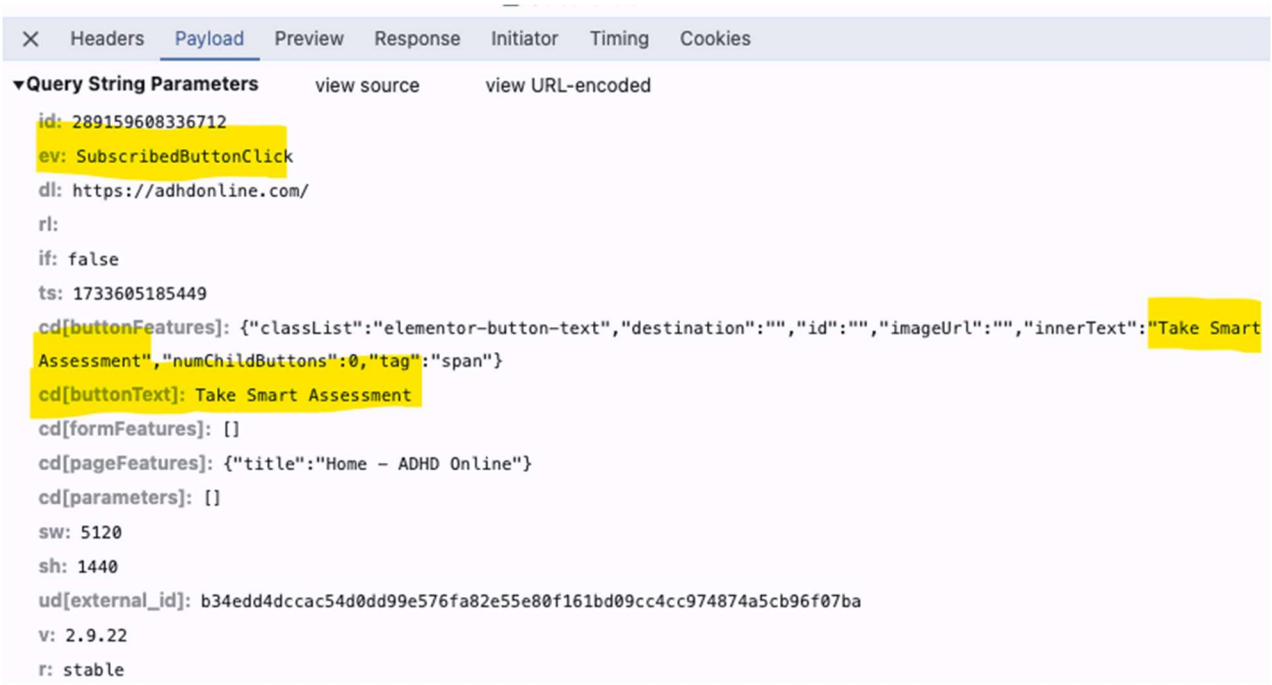
78. When individuals visit ADHD Online's Website via an HTTP request to ADHD Online's server, ADHD Online's server sends an HTTP response that displays the webpage visible to the User.

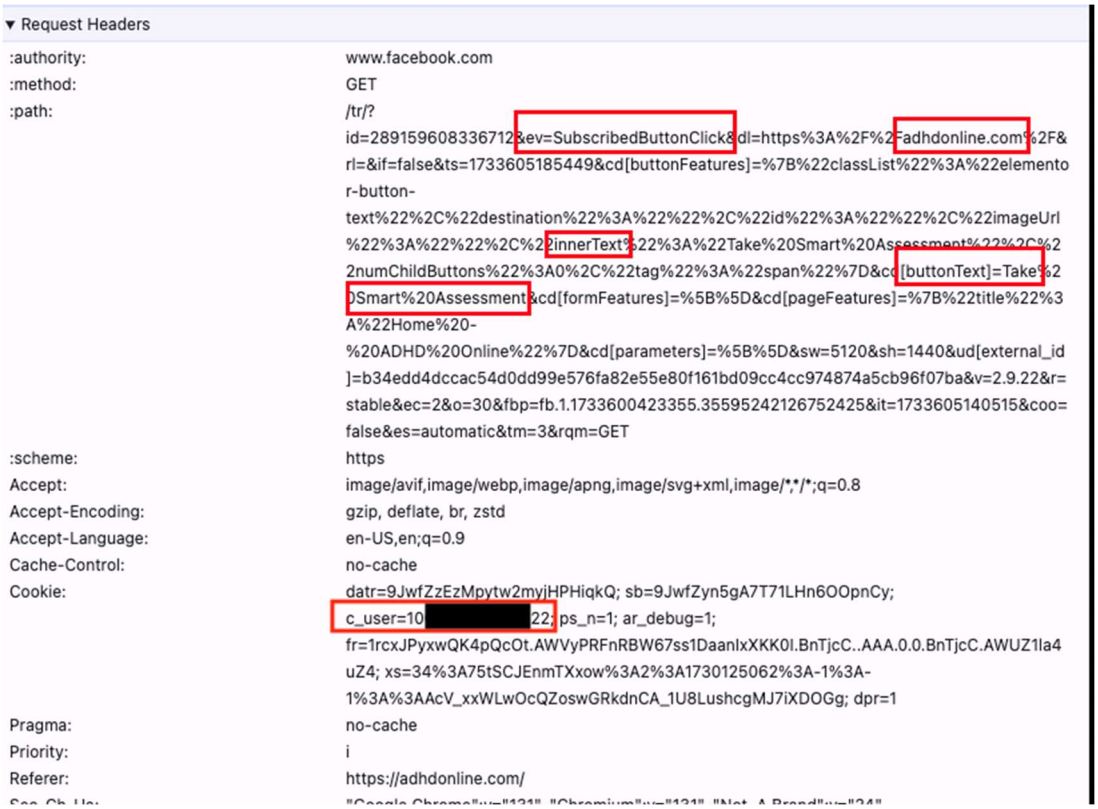
79. For example, when a User visits www.adhdonline.com, and clicks the "Take Smart Assessment" link, the User's web browser automatically sends an HTTP Request to Defendant's web server. The Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted in the first image below.

Figures 1-3: ***An HTTP single communication session sent from the device to Facebook that reveals the User's clicking on the button to "Take Smart Assessment" for ADHD diagnosis, through a "SubscribedButtonClick" event, along with the User's PII (including the c_user cookie which Meta uses to identify a particular Facebook user)[30]*****:**

[30] The c_user cookie is one of the ways Facebook identifies and tracks its users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has only one unique c_user cookie.


adhdonline.com
Scams - Phone, Mail...
Now offering Therapy in over 40 states! Find yours
ADHD Online
from Mentavi Health
Diagnosis
Treatment
Evidence-based mental healthcare personalized for you
We know that stewarding your mental health can be hard, especially if ADHD is part of your life. We're here to empower you with clinical insight and patient-focused care from assessment and diagnosis to treatment and beyond.
Get your diagnostic evaluation assessment for a one-time cost of $189
Take Smart Assessment


Headers
Payload
Preview
Response
Initiator
Timing
Cookies
▾Query String Parameters
view source
view URL-encoded
id: 289159608336712
ev: SubscribedButtonClick
dl: https://adhdonline.com/
rl:
if: false
ts: 1733605185449
cd[buttonFeatures]: {"classList":"elementor-button-text","destination":"","id":"","imageUrl":"","innerText":"Take Smart Assessment","numChildButtons":0,"tag":"span"}
cd[buttonText]: Take Smart Assessment
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Home – ADHD Online"}
cd[parameters]: []
sw: 5120
sh: 1440
ud[external_id]: b34edd4dccac54d0dd99e576fa82e55e80f161bd09cc4cc974874a5cb96f07ba
v: 2.9.22
r: stable



▼ Request Headers

:authority:	www.facebook.com
:method:	GET
:path:	/tr/? id=2891596083367128&ev=SubscribedButtonClick&dl=https%3A%2F%2Fadhdonline.com%2F& rl=&if=false&ts=1733605185449&cd[buttonFeatures]=%7B%22classList%22%3A%22elementor-button- text%22%2C%22destination%22%3A%22%22%2C%22id%22%3A%22%22%2C%22imageUrl %22%3A%22%22%2C%22innerText%22%3A%22Take%20Smart%20Assessment%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22span%22%7D&cd[buttonText]=Take%20Smart%20Assessment&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Home%20- %20ADHD%20Online%22%7D&cd[parameters]=%5B%5D&sw=5120&sh=1440&ud[external_id]=b34edd4dccac54d0dd99e576fa82e55e80f161bd09cc4cc974874a5cb96f07ba&v=2.9.22&r=stable&ec=2&o=30&fbp=fb.1.1733600423355.35595242126752425&it=1733605140515&coo=false&es=automatic&tm=3&rqm=GET
:scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	en-US,en;q=0.9
Cache-Control:	no-cache

Cookie:	datr=9JwfZzEzMpytw2myjHPHiqkQ; sb=9JwfZyn5gA7T71LHn6OOpnCy;
	c_user=10[redacted]22; ps_n=1; ar_debug=1;
	fr=1rcxJPyxwQK4pQcOt.AWVyPRFnRBW67ss1DaanIxXKK0I.BnTjcC..AAA.0.0.BnTjcC.AWUZ1la4uZ4; xs=34%3A75tSCJEnmTXxow%3A2%3A1730125062%3A-1%3A-
	1%3A%3AAcV_xxWLwOcQZoswGRkdnCA_1U8LushcgMJ7iXDOGg; dpr=1

Pragma:	no-cache
Priority:	i
Referer:	https://adhdonline.com/

80. Figures 2 and 3 depict the 'behind-the-scenes' source code that manipulates Users' browsers to capture and disclose their PHI and PII via the Pixel.

81. Facebook uses several cookies to identify users, including cookies named c_user, datr, fr, and _fbp.

82. If a User is a Facebook user, the information Facebook receives is linked to their Facebook profile (via their Facebook ID or "c_user id" cookie), which includes other identifying information about the user including pictures, personal interests, work history, relationship status, and other details.

83. The Facebook datr cookie identifies the web browser the User is using. It is an identifier unique to each User's specific web browser and is another way Meta can identify Facebook users (Facebook keeps a record of every datr cookie identifier associated with each of its users).

84. The Facebook fr cookie is an encrypted combination of the c_user and datr cookies.

85. ADHD Online also deposits cookies associated with third-parties such as Facebook and Google, but are disguised as first-party cookies.

86. Even if a user does not have a Facebook account or is not logged in to Facebook when browsing Defendant's Website, the Pixel transmits the User's web communications with Defendant's Website to Meta along with a unique identifier associated with another cookie called the "_fbp" cookie.

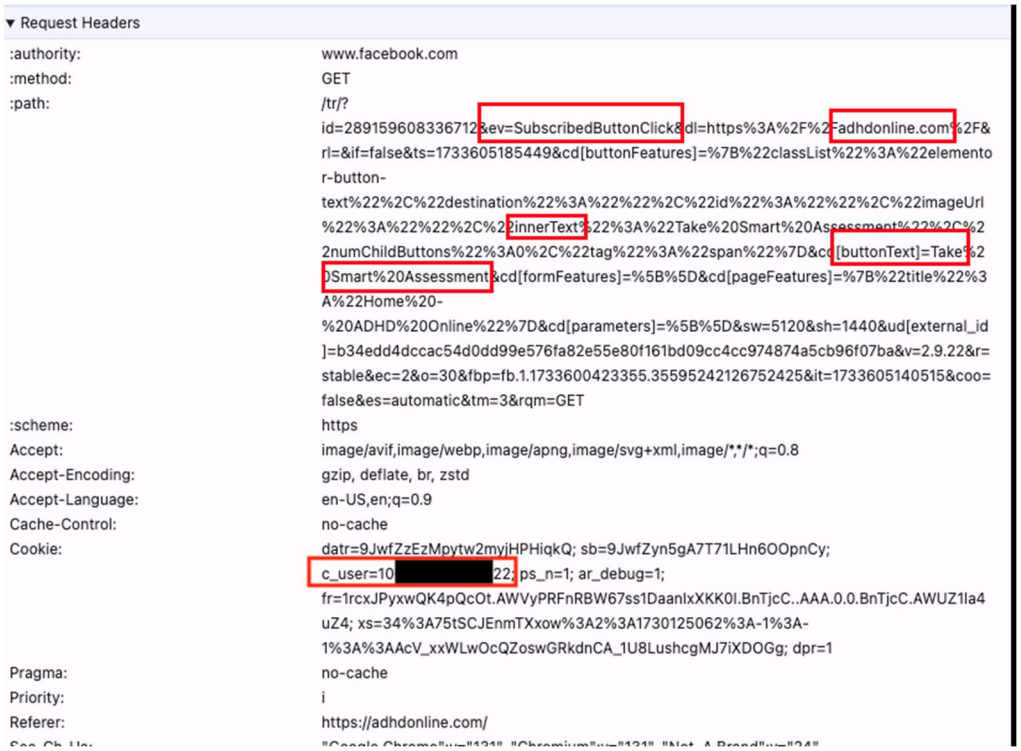
87. The _fbp cookie emanates from ADHD Online's Website as a putative first party cookie but is transmitted to Facebook through cookie-synching technology that hacks around the same-origin policy.

88. In this instance, ADHD Online begins tracking its Users from the moment they land on the Website, capturing PHI and PII including data that discloses the User's specific medical condition, the fact that the User is searching for specific treatments or doctors for their sensitive medical condition, that the User is taking a medical assessment for a specific medical condition, or that the User is signing up as patient of ADHD Online[31]—along with the User's unique Facebook ID, and other personal identifiers such as their device identifiers and their IP address.

[31] As discussed *infra*, each of these categories of information constitutes PHI.

89. Most worryingly, ADHD Online installed the Tracking Tools not only on its public-facing portion of the Website, but on its Patient Portal webpages as well.

90. At a minimum, the Meta Tracking Tools captured and disclosed that the User was seeking an assessment of their ADHD or ADHD-related conditions and symptoms, that they signed up as a patient of ADHD Online, and that they were seeking appointments with providers specializing in ADHD treatment, *see Figures 4-6* below*:*



▼ Request Headers

:authority:	www.facebook.com
:method:	GET
:path:	/tr/? id=2891596083367[redacted]&ev=SubscribedButtonClick&dl=https%3A%2F%2Fadhdonline.com%2F& rl=&if=false&ts=1733605185449&cd[buttonFeatures]=%7B%22classList%22%3A%22elemento r-button- text%22%2C%22destination%22%3A%22%22%2C%22id%22%3A%22%22%2C%22imageUrl %22%3A%22%22%2C%22innerText%22%3A%22Take%20Smart%20Assessment%22%2C%2 2numChildButtons%22%3A0%2C%22tag%22%3A%22span%22%7D&cd[buttonText]=Take%2 0Smart%20Assessment&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3 A%22Home%20- %20ADHD%20Online%22%7D&cd[parameters]=%5B%5D&sw=5120&sh=1440&ud[external_id]=b34edd4dccac54d0dd99e576fa82e55e80f161bd09cc4cc974874a5cb96f07ba&v=2.9.22&r= stable&ec=2&o=30&fbp=fb.1.1733600423355.35595242126752425&it=1733605140515&coo= false&es=automatic&tm=3&rqm=GET
:scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	en-US,en;q=0.9
Cache-Control:	no-cache

Cookie:	datr=9JwfZzEzMpytw2myjHPHiqkQ; sb=9JwfZyn5gA7T71LHn6OOpnCy;
	c_user=10[redacted]22; ps_n=1; ar_debug=1;
	fr=1rcxJPyxwQK4pQcOt.AWVyPRFnRBW67ss1DaanlxXKK0I.BnTjcC..AAA.0.0.BnTjcC.AWUZ1la4
	uZ4; xs=34%3A75tSCJEnmTXxow%3A2%3A1730125062%3A-1%3A-
	1%3A%3AAcV_xxWLwOcQZoswGRkdnCA_1U8LushcgMJ7iXDOGg; dpr=1

Pragma:	no-cache
Priority:	i
Referer:	https://adhdonline.com/

Figure 4. ***Example of a HTTP single communication session sent from the user's browser to Facebook that reveals the fact that the user started the ADHD Online "Smart Assessment," via the 'SubscribedButtonClick' event, and the user 's unique personal identifiers including the FID (c_user field).***

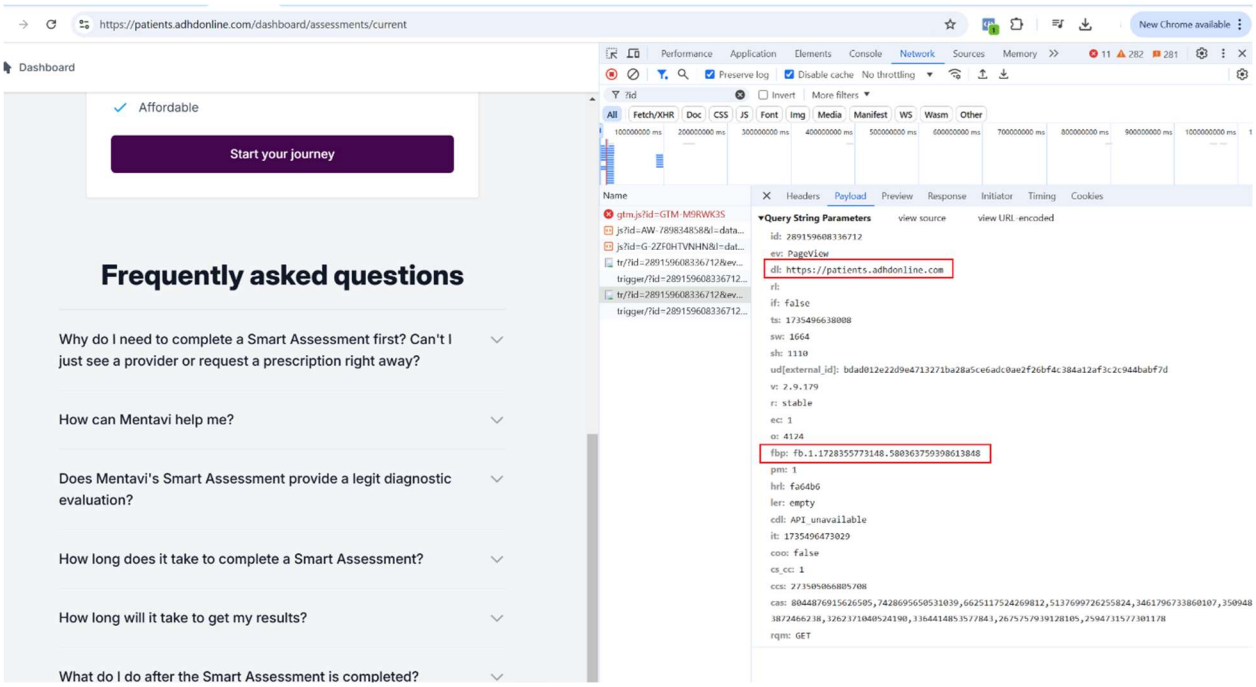


Figure 5. ***Defendant's Meta Pixel in the Patient Portal that reveals the User's patient status to Facebook.***

Figure 6. ***Example of a HTTP single communication session sent from the patient's browser to Facebook that reveals the fact that the patient is in the appointments section of the patient portal dashboard, along with the user's unique personal identifiers including the FID (c_user field).***

91. Consequently, when Users visit ADHD Online's Website and communicate their PHI and PII, this data is transmitted to Facebook including, but not limited to, health conditions experienced and treatments sought (mental health care), text of specific button/menu selections, and patient status. Additional collected and conveyed information includes instances when patients self-enroll in the patient portal and/or access their portal via a designated button (or link) on the Website. Each of these activities involves the transmission of sensitive information—such as unique personal identifiers and portal usage data—which is inevitably communicated to Facebook (and likely other third parties).

92. While Defendant currently limited its Meta Pixel's collection of patients' PHI and PII, upon information and good faith belief, ADHD Online's Meta Pixel tracked its registered Users as they set up an account, filled out medical assessments, and looked for specific ADHD treatments.[32]

93. Once Facebook has that data, it processes, analyzes, and assimilates it into databases like Core Audiences or Custom Audiences for advertising purposes. If the website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies the user's name and Facebook profile.

94. In sum, the Pixel allows Facebook to learn, manipulate, and use for financial gain, the medical and private content Defendant's Website Users communicated, viewed, or otherwise interacted with on Defendant's Website.

[32] The full scope of Defendant's interceptions and disclosures of Plaintiffs' communications to Meta and Google can only be determined through formal discovery. However, given that Defendant did choose to embed third-party Tracking Tools on the log-in and sign up pages for the patient portal, as well as within the portal, upon information and good faith belief Plaintiff alleges that ADHD was collecting PHI and PII from patients in the portal beyond what the Tracking Tools are collecting currently.

D. Google Tracking Tools

95. Alphabet Inc., the parent holding company of Google, generates revenue primarily by delivering targeted online advertising through Google, which is the creator of Google's source code and an established advertising company.

96. Like Meta, Google creates code—associated with Google's advertising system and products, including Google Analytics— that website developers can install on their websites to track user activity. Whenever a user visits a website that is running Google tracking code, Google's code directs the user's browser to send a separate and concurrent communication to Google without the user's knowledge.

97. The information that is intercepted and transmitted to Google via the Google tracking code includes: (i) the URL of the specific webpage a user is trying to access; (ii) the user's IP address; (iii) the User-agent, which identifies the user's device platform and browser; (iv) the user's geolocation, if available; (v) the Referrer, which is the URL of the page on which the user clicked a link to access a new page; (vi) event data, which describes how users interact with a website, for example, whether they saw an ad or played a video; and (vii) actual search queries on the site.

98. Google tracking code tells Google exactly what a user's browser communicated to the website.

99. Like the Meta Pixel, Google associates the information it obtains via Google's source code with other information about the user, using personal identifiers that are transmitted concurrently with other information the code is configured to collect. These identifiers include the "cid," a combination of the time the user visited the website and a unique identifier. The "cid" is assigned to an individual's browser and can persist for up to two years, allowing Google to link a

series of events to the same browser and, thus, to an individual. For Google account holders this identifier is also linked to that account.

100. Google DoubleClick is an advertising service that records internet users' viewing habits across the web, collecting information about their interests and tastes that includes the things they buy and the websites they visit, and uses several tools including cookies placed in users' browsers, to personally identify these "profiles of viewing habits" by linking them to specific individuals.[33]

101. Information sent to Google is sent alongside the users' unique identifier (such as the "cid" cookie from Google Analytics and DSID or IDE cookies from Google DoubleClick), thereby allowing individual patients' communications with ADHD Online, and the PHI and PII contained in those communications, to be linked to their unique Google accounts and therefore their identity.[34]

102. Similar to the way that Facebook's _fbp cookie operates, Google Analytics also uses certain "first-party" cookies like _ga and _gid to track users' activities on non-Google websites.

103. In addition to information gleaned from a user's unique ID, Google can create a unique, digital "fingerprint" for a user based on data transmitted via Google Source Code, which allows Google to link certain web activity to a user.

104. This "fingerprint" can consist of information regarding a user's screen depth, screen resolution, browser name and version, and operating system name and version, as well as a user's

[33] *See*, *e.g., Double Trouble*, Electronic Privacy Information Center (March 21, 2000), https://archive.epic.org/privacy/doubletrouble/

[34] *See Brown v. Google LLC*, 685 F. Supp. 3d 909 (N.D. Cal. 2023) (quoting Google employee deposition testimony explaining how Google tracks user data).

Internet Protocol ("IP") address.

105. With that information, Google can link data acquired through Google Analytics or DoubleClick to a particular user.[35]

106. Browser-fingerprints are also considered personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors.[36]

107. After tracking, intercepting, and acquiring user's information, Google uses the information for personalized advertising in its advertising systems which includes, but is not limited to, Google Analytics and DoubleClick.

108. For example, Google Analytics uses the information it collects to facilitate its Audience Targeting feature. Audience Targeting refers to serving ads to only a select number of users who share certain common characteristics.

109. For Google's Audience Targeting, Google can target ads to either "Pre-defined Google Audiences" or "Advertiser-curated Audiences." Pre-defined Audiences are those created by Google based on interest and demographic data. Advertiser-curated Audiences are customized audiences created by Google through the use of the Source Code, including audiences created through Google Analytics.

110. Like Meta, Google is therefore able to monetize the information surreptitiously intercepted, with Mindful Care's help, from visitors to Defendant's Web Properties.

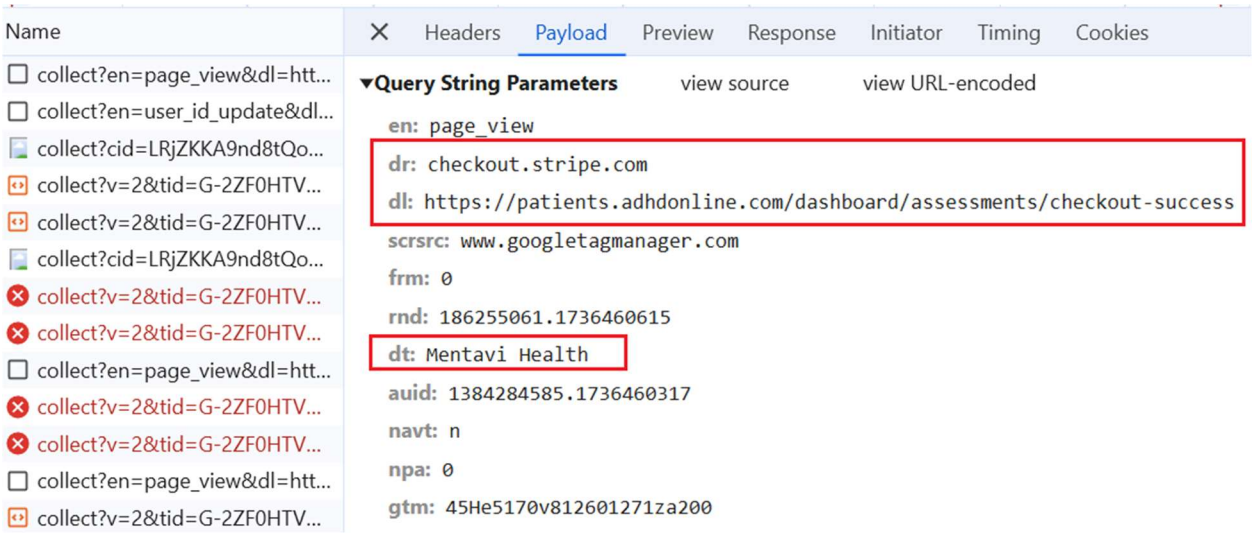
111. Google logs a user's browsing activities on non-Google websites and uses this data

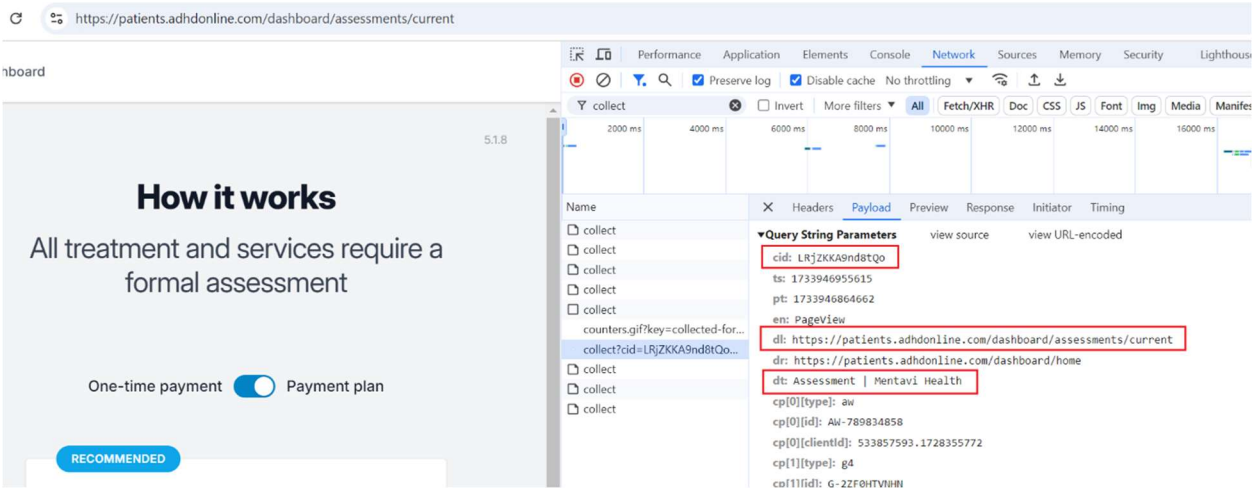
[35] In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users. *See* https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/.

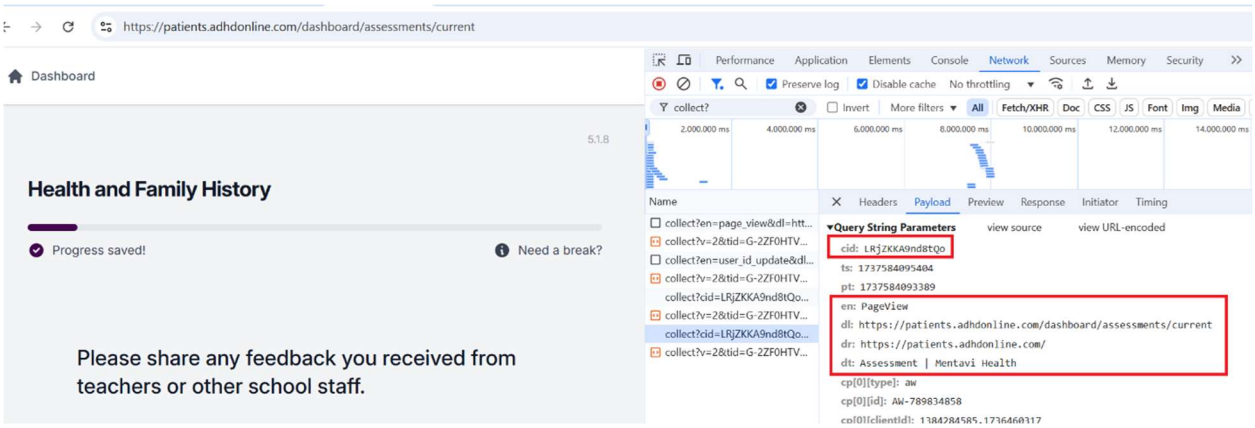
[36] Browser-fingerprints are protected personal identifiers under HIPAA. *See* 45 C.F.R. § 164.514(b)(2)(i)(M), (R).

for serving personalized ads.

112. Google Tracking Tools installed on the ADHD Online Website also collect sensitive PHI and PII from Defendant's patients. For example, Google trackers also capture and disclose that the user has signed up as a patient of ADHD Online, that they have paid to take Defendant's ADHD assessment, and the fact that they are taking the assessment, *see Figures 7-9 below:*







113. As described *supra*, this information is shared with Google along with the cid, IDE, DSID, __ga and _gid cookies which are used by Google to identify a particular user.

114. Based on the above examples of how the Tracking Tools operate on ADHD Online's Website, Meta and Google would know (i) that a particular individual—who Meta and Google could identify based on their respective accounts—was a patient or prospective patient of Defendant seeking mental healthcare services for their specific medical condition or symptoms, (ii) that the named patient searched for (or selected from Defendant's medical services) information regarding their specific medical condition, and (iii) that the patient in question was signing up for mental health services (and, upon information and belief, to make an appointment with a doctor).

115. Meta and Google would also know the named patient's location and IP address, among other identifiers associated with the patient's computer or cell phone.

116. Using this PHI and PII, technology companies can put the named patient into a Core or Custom Audience for purposes of targeted advertising by ADHD Online or any other company seeking to advertise its services or products to individuals that fit the named patient's profile.

117. Defendant, Meta, Google, and other third parties profit off of Plaintiffs' and Class

Members' PHI and PII without their knowledge, consent, or authorization.

118. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (a) embedded and implemented the Tracking Tools, which surreptitiously intercepted, recorded, and disclosed Plaintiffs' and other patients' and prospective patients' confidential communications and private information; (b) disclosed patients' and prospective patients' protected information to Meta and Google—unauthorized third parties; and (c) failed to provide notice to or obtain the consent from Plaintiffs and Class Members to share their PHI and PII with others.

E. ADHD Online's Use of the Tracking Tools Violated Its Own Privacy Policies.

119. ADHD Online breached Plaintiffs' and Class Members' right to privacy by unlawfully disclosing their PHI and PII to Facebook and Google.

120. Specifically, Plaintiffs and Class Members had a reasonable expectation of privacy based on ADHD Online's own representations to Plaintiffs and the Class that ADHD Online would not disclose their PHI and PII to third parties.

121. ADHD Online did not ask Users, including Plaintiffs, whether they consent to be wiretapped via the Pixel or to external sharing of their PHI and PII prior to submitting it to Defendant. Users are never told that their electronic communications are being wiretapped via the Tracking Tools.

122. ADHD Online's Privacy Policy does not state that Users' PHI and PII would be shared with Facebook or other unauthorized third parties.

123. ADHD Online recognizes that it collects sensitive patient data, including their health information and emphasizes its commitment to protecting patients' health data by adhering to strict security safeguards. Defendant states that "[a]ll such health information is handled

according to all applicable ethical and legal requirements, including state and federal laws and regulations."[37]

124. Moreover, ADHD Online's Privacy Policy recognizes that certain information they collect is PHI under HIPAA, and they may be a "business associate" subject to HIPAA.[38]

125. ADHD Online further promises that:

> [A]ny medical or health information that you provide that is subject to specific protections under applicable state laws (collectively, with PHI, "Protected Information"), will be used and disclosed in accordance with such applicable laws
> . . .
> If we collect, use, and discloses [sic] Protected Information on behalf of your Medical Group or Provider, such processing on behalf of your Medical Group or Provider shall be consistent with the Notice of Privacy Practices and as permitted in our agreements with the Medical Groups or Provider, except to the extent you have expressly authorized additional uses and disclosures.[39]

126. ADHD Online's Privacy Policy does not permit it to share patients' PHI for marketing purposes without authorization.[40]

127. While the ADHD Online's Privacy Policy discloses their use of cookies and pixels, it does not disclose that these tracking tools capture and share Users' PHI without the Users' consent.[41]

128. Plaintiffs and Class Members did not authorize Defendants to disclose their PHI for marketing purposes to Facebook or Google.

---

[37] *See* ADHD Online's *Privacy Policy*, https://adhdonline.com/privacy-policy/

[38] *Id.*
[39] *Id.*
[40] *See id.*
[41] *See id.*

129. By engaging in this improper sharing of information without Plaintiffs' and Class Members' consent, ADHD Online violated its own Privacy Policy and breached Plaintiffs' and Class Members' right to privacy and unlawfully disclosed their PHI and PII.

F. ADHD Online's Use of the Tracking Tools Violates HIPAA.

130. Under federal law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient or household member of a patient for marketing purposes without the patients' express written authorization.

131. Guidance from HHS instructs healthcare providers that patient status alone is protected by HIPAA.

132. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

133. The Privacy Rule broadly defines protected health information as individually identifiable health information that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

134. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods

and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

> A. Names;
> …
> H. Medical record numbers;
> …
> J. Account numbers;
> …
> M. Device identifiers and serial numbers;
> N. Web Universal Resource Locators (URLs);
> O. Internet Protocol (IP) address numbers; … and
> P. Any other unique identifying number, characteristic, or code… and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

135. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

136. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI.

137. HHS has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[i]f such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."[42]

[42] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*,

138. Consistent with this restriction, HHS has issued guidance that provides, "[w]ith limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list."[43]

139. Here, as described, *supra*, ADHD Online provided patient information to third parties in violation of the Privacy Rule and its own Privacy Policy.

140. HIPAA also requires ADHD Online to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(c), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights," 45 C.F.R. § 164.312(a)(1) – which ADHD Online failed to do.

141. ADHD Online further failed to comply with other HIPAA safeguard regulations as follows:

a. Failing to ensure the confidentiality and integrity of electronic PHI that ADHD Online created, received, maintained and transmitted in violation of 45 C.F.R. section 164.306(a)(1);

b. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

[43] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html.

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to ADHD Online in violation of 45 C.F.R. section 164.308(a)(6)(ii);

d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);

e. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3), and

f. Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

142. Commenting on a June 2022 report discussing the use of Meta Pixels by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it … It is quite likely a HIPAA violation."[44]

143. ADHD Online's placing of a third-party tracking code on their Website is a violation of Plaintiffs' and Class Members' privacy rights under federal law. While Plaintiffs do not bring a claim under HIPAA itself, this violation demonstrates ADHD Online's wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

G. ADHD Online Violated Industry Standards.

144. It is a cardinal rule that a medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship.

[44] '*Deeply Troubled*': *Security experts worry about Facebook trackers on hospital sites*, ADVISORY BOARD, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers.

145. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

146. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)[.]

147. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

148. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping ethics guidelines for confidentiality.[45]

149. ADHD Online's use of the Tracking Tools also violates FTC data security guidelines. The FTC has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices.

[45] AMA Principles of Medical Ethics: I, IV, *Chapter 3: Opinions on Privacy, Confidentiality & Medical Records*, https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf.

150. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*[46] established cyber-security guidelines for businesses. These guidelines state that businesses should protect the personal patient information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network vulnerabilities and implement policies to correct any security problems.

151. In fact, the FTC has recently brought enforcement actions against several healthcare companies, including Premom, BetterHelp, GoodRx and Flow Health for conveying information—or enabling an inference—about their consumers' health to unauthorized third parties without the consumers' consent.

152. Like the telehealth companies fined by the FTC in recent years, ADHD Online failed to implement these basic, industry-wide data security practices.

H. Users' Reasonable Expectation of Privacy.

153. Plaintiffs and Class Members were aware of ADHD Online's duty of confidentiality when they sought medical services from ADHD Online.

154. Indeed, when Plaintiffs and Class Members provided their PHI and PII to ADHD Online, they each had a reasonable expectation that the information would remain confidential and that ADHD Online would not share the PHI and PII with third parties for a commercial purpose, unrelated to patient care.

155. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

[46] *See* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

156. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[47]

157. Personal data privacy and obtaining consent to share PHI and PII are material to Plaintiffs and Class Members.

I. Unique Personal Identifiers are PHI.

158. While not all health data is covered under HIPAA, the law specifically applies to healthcare providers, health insurance providers and healthcare data clearinghouses.[48]

159. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered personally identifiable information ("PII"). This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual.

160. These HIPAA Identifiers, as relevant here, include dates related to an individual, their device identifiers, web URLs and IP addresses.[49]

---

[47] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/.

[48] *See* Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook*, The Markup (June 21, 2022), https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook (stating that "[w]hen you are going to a covered entity's website, and you're entering information related to scheduling an appointment, including your actual name, and potentially other identifying characteristics related to your medical condition, there's a strong possibility that HIPAA is going to apply in those situations").

[49] *Guidance regarding Methods for De-identification of Protected Health Information in*

161. Unique personal identifiers become PHI when they can be associated with personal health information.[50]

162. ADHD Online improperly disclosed Plaintiffs' and Class Members' HIPAA identifiers, including the dates they sought treatments, their computer IP addresses, device identifiers and web URLs visited to Facebook and Google through their use of the Tracking Tools *in addition to* services selected, patient statuses, medical conditions, and treatments sought.

163. An IP address is a number that identifies the address of a device connected to the Internet. IP addresses are used to identify and route communications on the Internet. IP addresses of individual Internet users are used by Internet service providers, websites and third-party tracking companies to facilitate and track Internet communications.

164. Facebook tracks every IP address associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

165. Facebook, Google and other third-party marketing companies track IP addresses to target individual homes and their occupants with advertising.

166. Under HIPAA, an IP address is considered personally identifiable information, which is defined as including "any unique identifying number, characteristic or code" and specifically listing IP addresses among examples. *See* 45 C.F.R. § 164.514 (2).

167. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other

---

Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

[50] *See id.* ("[p]rotected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.").

information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

168. Consequently, ADHD Online's disclosure of Plaintiffs' and Class Members' IP addresses violated HIPAA and industry-wide privacy standards because it was connected to their past, present, or future medical conditions and treatment.

J. ADHD Online Was Enriched & Benefitted from the Use of Tracking Tools that Enabled the Unauthorized Disclosures Alleged Herein

169. One of the primary reasons that ADHD Online decided to embed Tracking Tools on their Website was to improve marketing through creating campaigns that maximize conversions (thereby decreasing ADHD Online's costs and boosting its revenues).

170. After receiving individually identifiable patient health information communicated on the ADHD Online Website, Meta and Google forward this data, and its analysis of this data, to ADHD Online.

171. ADHD Online then uses this data and analysis for its own commercial purposes that include understanding how Users utilize their Website. ADHD Online also receives an additional commercial benefit from using tracking tools such as the Meta Conversions API, and Google Analytics, namely being able to serve more targeted advertisements to existing and prospective patients on Facebook and Instagram.

172. Facebook advertises its Pixel as a piece of code "that can help you better understand the ***effectiveness of your advertising*** and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting. And when you

use the Conversions API alongside the Pixel, it creates a more reliable connection that helps the delivery system ***decrease your costs***."[51]

173. Retargeting is a form of online marketing that targets Users with ads based on previous internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[52]

174. In the healthcare context the process of increasing conversions and retargeting occurs by sending a successful action on a health care website back to a third party data broker like Facebook or Google via the tracking technologies embedded on, in this case, ADHD Online's website. For example, if a new patient signs up to use ADHD Online's services, their information is sent to Facebook. Facebook can then use its data on the User to find more users to click on an ADHD Online ad and ensure that those users targeted are more likely to convert.[53]

175. Similarly, Google retargets web users via its remarketing ads, by using trackers that add the user to a remarketing list after they visit a website, and serving them the ads on websites that use the Google Ad network, to entice them to return and complete a transaction.[54] Google

[51] *What is the Meta Pixel,* https://www.facebook.com/business/tools/meta-pixel (emphasis added).

[52] *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/.

[53] *See, e.g.*, *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), *https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking*.

[54] Intuit MailChimp, *Google Remarketing*, https://mailchimp.com/marketing-glossary/google-remarketing/

promotes its "remarketing" services as highly personalizable, cost-effective, and proven to convert users to customers.[55]

176. During this process, the Tracking Tools load and capture as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Tracking Tools capture "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[56]

177. Plaintiffs' and Class Members' PHI and PII has considerable value as highly monetizable data, especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

178. In exchange for disclosing the PHI and PII of their account holders and patients, ADHD Online is compensated by Facebook and Google in the form of enhanced advertising services and more cost-efficient marketing on their platform.

179. But companies have started to warn about the potential HIPAA violations associated with using pixels and Tracking Tools because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.[57]

180. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data

---

[55] *See id*.

[56] *https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking*..

[57] *See The guide to HIPAA compliance in analytics,* https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant).

vacuum sending PHI to Meta servers," and "[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[58]

181. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[59]

182. Whether a User has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court has recognized that the pixels' ability to track comprehensive browsing history is also relevant. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from Websites and Google Cookies that it collects across the internet on the same user).

183. ADHD Online retargeted patients and potential patients to get more people to purchase their services. These patients include Plaintiffs and Class Members.

184. Thus, utilizing Tracking Tools directly benefits ADHD Online by, among other things, reducing the cost of advertising and retargeting.

K. Plaintiffs' PHI and PII is Extremely Valuable.

185. Plaintiffs' and Class Members' PHI and PII had value, and ADHD Online's disclosure and interception harmed Plaintiffs and the Class by not compensating them for the value of their PHI and PII and, in turn, decreasing the value of their PHI and PII.

---

[58] *How To Make Facebook Ads HIPAA Compliant And Still Get Conversion Tracking*, *supra* note 59.

[59] *The complex world of healthcare retargeting, supra*, note 52.

186. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

187. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

188. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[60]

189. A 2015 article from TechCrunch accurately noted that "[d]ata has become a strategic asset that allows companies to acquire or maintain a competitive edge."[61] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

190. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data (after costs).[62] That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

191. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend.

---

[60] *See* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[61] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

[62] *See What Your Data is Really Worth to Facebook* (July 12, 2019), https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/.

Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[63]

192. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[64]

193. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

194. Courts recognize the value of PHI and PII and the harm when it is disclosed without consent. *See, e.g., In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

195. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

---

[63] Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055, 2056-57 (2004).

[64] *See* Kevin Mercadante, *10 Apps for Selling Your Data for Cash*, Wallet Hacks (Nov. 18, 2023), https://wallethacks.com/apps-for-selling-your-data/.

196. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

197. The value of health data is well-known and various reports have been conducted to identify its value.

198. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[65]

199. Trustwave Global Security published a report entitled *The Value of Data*. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[66]

200. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[67]

---

[65] *See Valuing Healthcare Data,* The Value Examiner (July/Aug. 2023), https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf.

[66] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

[67] *See* https://time.com/4588104/medical-data-industry/.

201. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[68]

202. The dramatic difference in the price of healthcare data compared to other forms of PHI and PII commonly sold is evidence of the value of PHI.

203. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

204. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

205. ADHD Online gave away Plaintiffs' and Class Members' communications and transactions on its Digital Platforms without permission.

206. The unauthorized access to Plaintiffs' and Class Members' personal and PHI and PII has diminished the value of that information, resulting in harm to Website Users, including Plaintiffs and Class Members.

207. Plaintiffs have a continuing interest in ensuring that their future communications with ADHD Online are protected and safeguarded from future unauthorized disclosure.

[68] *See* Christina Farr, *Hospital execs say they are getting flooded with requests for your health data*, CNBC (Dec. 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff Martinez

208. Beginning in or around early 2022 and most recently in late 2023, Plaintiff Martinez utilized ADHD Online's Website on her personal electronic devices to create an account on the patient portal, provide personal and medical information and history, and to diagnose and seek treatment for ADHD.

209. While seeking services and treatments, ADHD Online required Plaintiff Martinez to provide—and Plaintiff Martinez provided— PHI and PII including her name, email address and medical conditions and history, including PTSD, bipolar, depression, and autism. Additionally, ADHD Online required Plaintiff to provide additional PHI, including weight, height, whether she was on medications including mood stabilizers, and which of their services she wanted to use.

210. While searching ADHD Online's specific services, the Website presented numerous guided questions and asked Plaintiff to respond to those questions to confirm its hypothesis of her condition. For Plaintiff's conditions, ADHD Online required Plaintiff to provide information regarding her medications and then asked her personal questions regarding past trauma and medical history.

211. While Plaintiff Martinez was a User of ADHD Online's services, she never consented to or authorized the use of her PHI and PII by third parties or to ADHD Online enabling third parties to access, interpret and use such PHI and PII.

212. Plaintiff Martinez had active Google and Facebook accounts while she used ADHD Online's services and she accessed ADHD Online's Website while logged into her Google and Facebook accounts on the same device.

213. After providing PHI and PII to ADHD Online through the Website, Plaintiff Martinez began seeing targeted health ads as she scrolled through her Facebook account, including ads for ADHD treatment.

214. Plaintiff Martinez trusted that the PHI and PII that she provided to Defendant would be safeguarded according to Defendant's policies, industry standards, and state and federal law.

215. Plaintiff Martinez was injured by Defendant's unauthorized disclosure of her confidential PHI and PII. Defendant's actions subjected her to unsolicited targeted advertising related to her specific medical conditions and caused significant mental distress arising from the implication that advertisers were aware of her medical conditions and the fear that her friends, family, or colleagues might see these advertisements and thereby learn of her medical conditions.

216. Additionally, Plaintiff lost the benefit of her bargain with Defendant. Plaintiff Martinez created an account with Defendant and used Defendant's Website to purchase prescriptions believing that Defendant would keep his PHI and PII confidential and would not have done so had she known of Defendant's actual practices. Finally, Defendant's practice of sharing Plaintiff's PHI and PII has diminished its value.

Plaintiff Parrish

217. Beginning in or around early 2018 and most recently in November 2022, Plaintiff Parrish utilized ADHD Online's Website on her personal electronic devices to provide personal and medical information and history, and to diagnose and seek treatment for ADHD.

218. While seeking services and treatments, ADHD Online required Plaintiff Parrish to provide—and Plaintiff Parrish provided— PHI and PII including her name, email address and medical conditions and history, including answering questions about her symptoms that may be related to ADHD. Additionally, ADHD Online required Plaintiff to provide additional PHI,

including weight, height, blood pressure, whether she was on medications and, if so, which ones, and which of their services she wanted to use.

219. While searching ADHD Online's specific services, the Website presented numerous guided questions and then Plaintiff to respond to questions to confirm its hypothesis of her condition. For Plaintiff's conditions, ADHD Online required Plaintiff to provide information regarding her medications and then asked her personal questions regarding past trauma and medical history.

220. Plaintiff Parrish also used the Website to make appointments, pay for medical services, and to get prescribed medication such as Adderall to treat her for ADHD.

221. While Plaintiff Parrish was a User of ADHD Online's services, she never consented to or authorized the use of her PHI and PII by third parties or to ADHD Online enabling third parties to access, interpret and use such PHI and PII.

222. Plaintiff Parrish had active Google and Facebook accounts while she used ADHD Online's services and she accessed ADHD Online's Website while logged into her Google and Facebook accounts on the same device.

223. After providing PHI and PII to ADHD Online through the Website, Plaintiff Parrish began seeing targeted health ads as she scrolled through her Facebook account, including ads for ADHD treatment and medication.

224. Plaintiff Parrish trusted that the PHI and PII that she provided to Defendant would be safeguarded according to Defendant's policies, industry standards, and state and federal law.

225. Plaintiff Parrish was injured by Defendant's unauthorized disclosure of her confidential medical information. Defendant's actions subjected her to unsolicited targeted advertising related to her specific medical conditions and caused significant mental distress arising

from the implication that advertisers were aware of her medical conditions and the fear that her friends, family, or colleagues might see these advertisements and thereby learn of her medical conditions.

226. Additionally, Plaintiff lost the benefit of her bargain with Defendant. Plaintiff Parrish created an account with Defendant and used Defendant's website to purchase prescriptions believing that Defendant would keep his PHI and PII confidential and would not have done so had she known of Defendant's actual practices. Finally, Defendant's practice of sharing Plaintiff's PHI and PII has diminished the value of the disclosed PHI and PII.

TOLLING

227. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know—and had no way of knowing—that their PHI and PII was intercepted and unlawfully disclosed to Facebook or Google because ADHD Online kept this information secret.

228. Plaintiffs did not learn of Defendant's intercepting of their activities and communications on Defendant's Website until being informed by the undersigned counsel of record shortly before this complaint was filed.

229. Plaintiffs had no reason to believe their PHI and PII was being intercepted through Defendant's Website, let alone in real time while Plaintiffs were inputting information into Defendant's Website but before Plaintiffs submitted their application. As detailed above, Defendant's privacy policy did not disclose that Defendant was sharing their information with Facebook or Google. Furthermore, the technologies Defendant embedded on their Website are not visible to the reasonable user—they are invisible and work in the background.

230. As a result, any and all applicable statutes of limitations otherwise applicable to the allegations herein have been tolled.

CLASS ACTION ALLEGATIONS

231. This action is brought by the named Plaintiffs on their behalf and on behalf of a proposed Class of all other persons similarly situated under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3) and 23(c)(4).

232. The Class that Plaintiffs seek to represent is defined as follows:

> All persons residing in the United States whose PHI and PII was disclosed to a third party without authorization or consent through Tracking Tools on ADHD Online's Website.

233. Excluded from the proposed Class are any claims for personal injury, wrongful death or other property damage sustained by the Class; and any Judge conducting any proceeding in this action and members of their immediate families.

234. Plaintiffs reserve the right to amend the definitions of the Class or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded or otherwise modified.

235. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. There are at least 1 million patients that have been impacted by ADHD Online's actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of ADHD Online.

236. **Commonality.** Common questions of law or fact arising from ADHD Online's conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class Members. These common questions include, but are not limited to, the following:

a) Whether and to what extent ADHD Online had a duty to protect the PHI and PII of Plaintiffs and Class Members;

b) Whether ADHD Online had duties not to disclose the PHI and PII of Plaintiffs and Class Members to unauthorized third parties;

c) Whether ADHD Online violated its own privacy policy by disclosing the PHI and PII of Plaintiffs and Class Members to Facebook and Google;

d) Whether ADHD Online adequately, promptly and accurately informed Plaintiffs and Class Members that their PHI and PII would be disclosed to third parties;

e) Whether ADHD Online violated the law by failing to promptly notify Plaintiffs and Class Members that their PHI and PII was being disclosed without their consent;

f) Whether ADHD Online adequately addressed and fixed the practices which permitted the unauthorized disclosure of patients' PHI and PII;

g) Whether ADHD Online engaged in unfair, unlawful or deceptive practices by failing to keep the PHI and PII belonging to Plaintiffs and Class Members free from unauthorized disclosure;

h) Whether ADHD Online violated the federal and state statutes asserted as claims in this Complaint;

i) Whether Plaintiffs and Class Members are entitled to actual, consequential and nominal damages as a result of ADHD Online's wrongful conduct;

j) Whether ADHD Online knowingly made false representations as to their data security and privacy policy practices;

k) Whether ADHD Online knowingly omitted material representations with respect to their data security and privacy policy practices; and

l) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of ADHD Online's disclosure of their PHI and PII.

237. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PHI and PII, like that of every other Class Member, was compromised as a result of ADHD Online's incorporation and use of the Tracking Tools.

238. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class, and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

239. **Predominance.** ADHD Online has engaged in a common course of conduct toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data was unlawfully stored and disclosed to unauthorized third parties, including Facebook and Google, in the same way. The common issues arising from ADHD Online's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

240. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would, therefore, have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for ADHD Online. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

241. **Policies Generally Applicable to the Class.** ADHD Online has acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief and corresponding declaratory relief are appropriate on a class-wide basis.

242. **Ascertainability & Notice.** Membership in the Class can be determined by objective records maintained by ADHD Online, and adequate notice can be given to Class Members directly using information maintained in ADHD Online's records.

243. **Class-wide Injunctive Relief.** Unless a Class-wide injunction is issued, ADHD Online may continue in its failure to properly secure the PHI and PII of Class Members, ADHD Online may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and ADHD Online may continue to act unlawfully as set forth in this Complaint as ADHD Online has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

244. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a) Whether ADHD Online owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing and safeguarding their PHI and PII and not disclosing it to unauthorized third parties;

b) Whether ADHD Online breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using and safeguarding their PHI and PII;

c) Whether ADHD Online failed to comply with their own policies and applicable laws, regulations and industry standards relating to data security;

d) Whether ADHD Online adequately and accurately informed Plaintiffs and Class Members that their PHI and PII would be disclosed to third parties;

e) Whether ADHD Online failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

f) Whether Class Members are entitled to actual, consequential and nominal damages and injunctive relief as a result of ADHD Online's wrongful conduct.

CAUSES OF ACTION

COUNT I

VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1), *et seq*.
Unauthorized Interception, Use and Disclosure
(*On Behalf of Plaintiffs & the Nationwide Class*)

245. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

246. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

247. The ECPA protects both sent and received communications.

248. The ECPA, specifically 18 U.S.C. § 2520(a), provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed or intentionally used in violation of Chapter 119.

249. The transmissions of Plaintiffs' and Class Members' PHI and PII to ADHD Online via ADHD Online's Website is a "communication" under the ECPA's definition under 18 U.S.C. § 2510(12).

250. The transmission of PHI and PII between Plaintiffs and Class Members and ADHD Online via their Website is a "transfer[s] of signs, signals, writing, … data, [and] intelligence of

[some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

251. The ECPA defines "content" when used with respect to electronic communications to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

252. The ECPA defines "interception" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

253. The ECPA defines "electronic, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies ADHD Online, Meta and Google use to track Plaintiffs' and Class Members' communications;
b. Plaintiffs' and Class Members' browsers;
c. Plaintiffs' and Class Members' computing devices;
d. ADHD Online's web-servers and
e. The Tracking Tools deployed by ADHD Online to effectuate the sending and acquisition of users' and patients' sensitive communications.

254. Plaintiffs and Class Members' interactions with ADHD Online's Website are electronic communications under the ECPA.

255. By utilizing and embedding the Tracking Tools and, upon information and belief, Conversions API on their Website and servers, ADHD Online intentionally intercepted, endeavored to intercept and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

256. Specifically, ADHD Online intercepted Plaintiffs' and Class Members' electronic communications via the Tracking Tools and Conversions API, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' PHI and PII to Facebook and Google.

257. Furthermore, Defendant intercepted the "contents" of Plaintiffs' communications in at least the following forms:

a. The parties to the communications;

b. PII such as patients' IP addresses, Facebook IDs, unique Google identifiers, browser fingerprints and other unique identifiers;

c. Patient communications about specific medical conditions;

d. The precise dates and times when patients click to Log-In on Defendant's Website;

e. Patient communications about specific treatments;

f. The precise text of specific buttons on Defendant's Website that patients click to exchange communications including mental health assessments;

g. Information that is a general summary or informs third parties of the subject of communications that Defendant sends back to patients in response to requests for information about specific conditions, treatments, payment and other information.

258. ADHD Online intercepted communications that included, but are not limited to, communications to/from Plaintiffs and Class Members regarding PHI and PII, including unique Facebook and Google IDs, IP addresses, and health information relevant to the screenings and treatment plans in which Plaintiffs and Class Members participated.

259. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Tools embedded and operating on their Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiffs' and Class Members' electronic communications to third parties, including Facebook

and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

260. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Tools embedded and operating on their Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs' and Class Members' electronic communications, for purposes other than providing health care services to Plaintiffs and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. *See* 18 U.S.C. § 2511(1)(d).

261. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Tools it embedded and operated on their Website, contemporaneously and intentionally redirected the contents of Plaintiffs' and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

262. ADHD Online intentionally used wire or electronic communications to increase its profit margins. ADHD Online specifically used the Tracking Tools and Conversions API to track and utilize Plaintiffs' and Class Members' PHI and PII for its own financial benefit.

263. ADHD Online was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communications.

264. Plaintiffs and Class Members did not authorize ADHD Online to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy via the Tracking Tools and Conversions API.

265. Any purported consent that ADHD Online received from Plaintiffs and Class Members was not valid.

266. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State—namely, violations of HIPAA, and invasion of privacy, among others.

267. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

268. Defendant is a "party to the communication" with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding and interception of Plaintiffs' and Class Members' PHI and PII does not qualify for the party exemption.

269. In sending and acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of ADHD Online's Website, creation of accounts, participation in ADHD Online's health screenings and purchasing a subscription plan, ADHD Online's purpose was tortious and designed to violate federal and state law, including as described above, a knowing intrusion into a private place, conversation or matter that would be highly offensive to a reasonable person.

270. ADHD Online's acquisition of patient communications that were used and disclosed to Facebook, Google, and other third parties was also done for purposes of committing

criminal and tortious acts in violation of the laws of the United States, as well as various common law causes of action.

271. Additionally, through the above-described Tracking Tools and intercepted communications, this information was, in turn, used by Facebook and Google to 1) place Plaintiffs in specific health-related categories and 2) target Plaintiffs with particular advertising associated with Plaintiffs' specific health conditions.

272. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing IIHI to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) ***relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual***, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[69]

273. Plaintiffs' information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiffs' expectations of privacy and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' PHI and PII for financial gain.

274. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

[69] § 1320d-(6) (emphasis added).

275. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it:

a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization and

b. Disclosed IIHI to Facebook and Google without patient authorization.

276. Defendant's conduct is subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Tracking Tools was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

277. Consumers have the right to rely upon the promises that companies make to them. ADHD Online accomplished its tracking through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that cause Meta Pixels and cookies (including but not limited to the fbp, _ga and _gid cookies) to be deposited on Plaintiffs' and Class Members' computing devices as "first-party" cookies that are not blocked.

278. The fbp, _ga, and _gid cookies, which constitute programs, commanded Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Facebook and Google and others.

279. Defendant knew or had reason to know that the fbp, _ga, and _gid cookies would command Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Facebook and Google.

280. Defendant's scheme or artifice to defraud consists of:

a. the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited in the claims below and

b. the placement of the 'fbp,' _ga and _gid cookies on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookies from Meta and Google.

281. As such, Defendant cannot viably claim any exception to ECPA liability.

282. As a direct and proximate result of ADHD Online's violation of the ECPA, Plaintiffs and Class Members were damaged by ADHD Online's conduct.

283. As a result of Defendant's violation of the ECPA, Plaintiffs and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT II

NEGLIGENCE
(*On Behalf of Plaintiffs & the Nationwide Class*)

284. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

285. Upon accepting, storing and controlling the PHI and PII of Plaintiffs and the Class, ADHD Online owed—and continues to owe—a duty to Plaintiffs and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive PHI and PII.

286. ADHD Online breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PHI and PII from unauthorized disclosure.

287. It was reasonably foreseeable that ADHD Online's failures to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PHI and PII through their use of the Tracking Tools and Conversions API would result in unauthorized third parties—such as Facebook and Google—gaining unlawful access to such PHI and PII.

288. ADHD Online's duty of care to use reasonable measures to secure and safeguard Plaintiffs' and Class Members' PHI and PII arose due to the special relationship that existed

between ADHD Online and its patients, which is recognized by statute, regulations and the common law.

289. In addition, ADHD Online had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

290. ADHD Online's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PHI and PII. ADHD Online's misconduct included the failure to (1) secure Plaintiffs' and Class Members' PHI and PII; (2) comply with industry-standard data security practices; (3) implement adequate Website and event monitoring and (4) implement the systems, policies and procedures necessary to prevent unauthorized disclosures resulting from the use of the Tracking Tools and Conversions API.

291. As a direct result of ADHD Online's breach of their duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class Members' PHI and PII, Plaintiffs and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

292. ADHD Online's wrongful actions and inactions and the resulting unauthorized disclosure of Plaintiffs' and Class Members' PHI and PII constituted (and continues to constitute) negligence at common law.

293. Plaintiffs and the Class are entitled to recover damages in an amount to be determined at trial.

COUNT III

BREACH OF IMPLIED CONTRACT
(*On Behalf of Plaintiffs & the Nationwide Class*)

294. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

295. As a condition of utilizing Defendant's Website and receiving services from Defendant's professionals, Plaintiffs and the Class Members provided their PHI and PII and compensation for their medical care.

296. When Plaintiffs and Class Members provided their data to ADHD Online in exchange for services, they entered into an implied contract pursuant to which ADHD Online agreed to safeguard and not disclose their PHI and PII without consent.

297. Plaintiffs and Class Members accepted ADHD Online's offers and provided their PHI and PII to ADHD Online.

298. By providing their PHI and PII and upon Defendant's acceptance of this information, Plaintiffs and Class Members (as one set of parties) and Defendant (as the other party) entered into implied-in-fact contracts to keep the provided information private and confidential.

299. This obligation was described in the terms that Defendant itself represented on its own Notice of Privacy Practices, which Defendant itself required Plaintiffs and Class Members assent to prior to proceeding with registration. Therefore, Defendant expressly assented to this obligation in these implied contracts.

300. Plaintiffs and Class Members would not have entrusted ADHD Online with their PHI and PII in the absence of an implied contract between them and ADHD Online obligating them not to disclose this PHI and PII without consent.

301. Defendant breached its obligations in the implied contracts by intercepting (or facilitating the interception of), disclosing and sharing with third parties the PHI and PII belonging to Plaintiffs and Class Members without their consent.

302. As a direct and proximate result of ADHD Online's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members would not have used ADHD Online's services or would have paid substantially for these services, had they known their PHI and PII would be disclosed.

303. Plaintiffs and Class Members are entitled to compensatory and consequential damages because of ADHD Online's breach of implied contract.

COUNT IV

BREACH OF CONFIDENCE
(*On Behalf of Plaintiffs & the Nationwide Class*)

304. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

305. Possessors of non-public medical information, such as ADHD Online, have a duty to keep such medical information completely confidential.

306. Plaintiffs and Class Members had reasonable expectations of privacy in the responses and communications entrusted to ADHD Online through their Website, which included highly sensitive PHI and PII.

307. Contrary to their duties as telehealth institutions and their express promises of confidentiality, ADHD Online installed the Tracking Tools and Conversions API to disclose and

transmit to third parties Plaintiffs' and Class Members' PHI and PII, including data relating to Plaintiffs' and Class Members' health.

308. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent or authorization.

309. The third-party recipients included, but may not be limited to, Facebook and Google.

310. As a direct and proximate cause of ADHD Online's unauthorized disclosures of Plaintiffs' and Class Members' PHI and PII, Plaintiffs and Class Members were damaged by ADHD Online's breach of confidentiality in that (a) sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private; (b) Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; (c) ADHD Online eroded the essential confidential nature of health services that Plaintiffs and Class Members participated in; (d) general damages for invasion of their rights in an amount to be determined by a jury at trial; (e) nominal damages for each independent violation; (f) the unauthorized use of something of value (the highly sensitive PHI and PII) that belonged to Plaintiffs and Class Members and the obtaining of a benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation to Plaintiffs or Class Members for the unauthorized use of such data; (g) diminishment of the value of Plaintiffs' and Class Members' PHI and PII; and (h) violation of property rights Plaintiffs and Class Members have in their PHI and PII.

COUNT V

UNJUST ENRICHMENT
(*On Behalf of Plaintiffs & the Nationwide Class*)

311. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

312. Plaintiffs bring this claim in the alternative to their common law causes of action.

313. By intercepting (or facilitating the interception of), disclosing and sharing with third parties the PHI and PII belonging to Plaintiffs and Class Members without their consent, Defendant benefitted (and was enriched) through, *inter alia*, receiving revenues from this conduct from parties that received and used this info such as Meta/Facebook.

314. Plaintiffs and Class Members conferred a benefit upon ADHD Online in the form of the monetizable PHI and PII that ADHD Online collected from them and disclosed to third parties, including Facebook and Google, without authorization and proper compensation.

315. ADHD Online consciously collected and used this information for their own gain, providing ADHD Online with economic, intangible and other benefits, including substantial monetary compensation.

316. ADHD Online unjustly retained those benefits at the expense of Plaintiffs and Class Members because ADHD Online's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs or Class Members.

317. This benefit was received at the expense of Plaintiffs and Class Members since their PHI and PII has diminished in value because of this disclosure.

318. The benefits that ADHD Online derived from Plaintiffs and Class Members were not offered by Plaintiffs or Class Members gratuitously and, thus, rightly belongs to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in New York and every

other state for ADHD Online to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts and trade practices alleged in this Complaint.

319. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

320. ADHD Online should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds that ADHD Online received, and such other relief as the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Classes, respectfully request that this Court enter an Order in their favor and against ADHD Online as follows:

a) Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiffs as representatives of the Classes, and appointing their counsel to represent the Classes;

b) For equitable relief enjoining ADHD Online from engaging in the wrongful conduct complained of herein pertaining to the misuse and unauthorized disclosure of Plaintiffs' and Class Members' PHI and PII;

c) For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

d) For an award of damages, including but not limited to, actual, consequential, punitive and nominal damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

f) Pre- and post-judgment interest on any amounts awarded; and

g) Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: February 27, 2025

Respectfully submitted,

s/: David S. Almeida
David S. Almeida
Bar # IL6285557
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (708) 529-5418
E: david@almeidalawgroup.com

Brandon M. Wise*
PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP
IL Bar # 6319580*
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
Ph: (314) 833-4825
bwise@peifferwolf.com

Andrew R. Tate*
PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP
GA Bar # 518068*
235 Peachtree St. NE, Suite 400
Atlanta, GA 30303
Ph: 404-282-4806
atate@peifferwolf.com

**Pro Hac Vice applications to be submitted*

Attorneys for Plaintiff & the Putative Class